Snell Advanced Media

Installation Guide

Media Transformer (ABR Streaming) V7.2

For sQ Server ISA-Only Systems

Information and Notices

Copyright and Disclaimer

Copyright protection claimed includes all forms and matters of copyrightable material and information now allowed by statutory or judicial law or hereinafter granted, including without limitation, material generated from the software programs which are displayed on the screen such as icons, screen display looks etc.

Information in this manual and software are subject to change without notice and does not represent a commitment on the part of SAM. The software described in this manual is furnished under a license agreement and can not be reproduced or copied in any manner without prior agreement with SAM or their authorized agents.

Reproduction or disassembly of embedded computer programs or algorithms prohibited.

No part of this publication can be transmitted or reproduced in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without permission being granted, in writing, by the publishers or their authorized agents.

SAM operates a policy of continuous improvement and development. SAM reserves the right to make changes and improvements to any of the products described in this document without prior notice.

Contact Details

Customer Support

For details of our **Regional Customer Support Offices** please visit the SAM website and navigate to Support/24/7-Support.

www.s-a-m.com/support/247-support/

Customers with a support contract should call their personalized number, which can be found in their contract, and be ready to provide their contract number and details.

 © 2017 SAM

Contents

Information and Notices 2
Copyright and Disclaimer 2
Contact Details 2

Media Transformer (ABR Streaming) Configuration 4
Overview 4
Prerequisites 4
Verifying the Correct Version of Windows 4
Upgrading 5
Media Transformer Setup 6
Configure Operating System 6
Install Transformer Software 7
License 7
Transformer Settings 8
License 8
Network 8
Network: Clipnet 9
Options 9
HTTP 10
Startup 10
QTube Settings 10
Server: Search 11
Essence: Audio 12
Essence: Video (PC) 13
Setting Group Area Constraints 13
IIS and Couch DB Setup 14
Install IIS and CouchDB 14
Security 14
Authentication 16
Search Service Setup 17
Search Service Overview 17
Web Server Port 17
ISA Settings 17
Customise Log Output 17
Install Search Service 18

Load Balancer Configuration 20
Install and Configure NLB 20
Add Network Load Balancing Tools Feature to Server A and Server B 20
Configure the Cluster 21
Install and Configure IIS 23
Add the Web Server (IIS) Role to the Servers 23
Configure IIS Shared Configuration on Server A and Server B 23
Change Default Web Site Bindings 24
Installing ARR manually without WebPI 24
Configure ARR 25
Create and configure a Server Farm 26
Force LBR Pass-through 31
Create and Configure Rewrite Rules 31

 © 2017 SAM

Media Transformer (ABR Streaming) Configuration

Overview

Prerequisites

To set-up the Media Transformer, the following is required:

- A working ISA sQ system that is configured to support a seat and has H.264 and/or MPEG-1 browse at 1.5 Mbit. The ISA system also needs the Search service installed.
- A newly installed Windows Server 2008 R2 64-bit operating system on an X8 motherboard.
- For convenience, customise the Windows Start menu to make Administrative Tools display on this menu.
- Sentinel Dongle Driver V7.4.2.exe
- Access to the Internet in order to download extra parts for IIS.
- An installer package containing Media Transformer and QTube Edit.
- A synchronised clock in order to successfully connect to remote shares.
- VC9 Redistributable (VC Runtime) must be installed.
- The PC client must be logged in as ‘Administrator’.

The previous options are usually set on installation by trained engineers with knowledge of Windows and networking. If in doubt, always contact SAM 24-Hour Support before changing any setting.

Verifying the Correct Version of Windows

Microsoft Windows Server 2008 R2 is different to Microsoft Windows Server 2008. Ensure that the correct Release 2 edition is being used.

1. Right-click on **Computer** and select **Properties**.
2. Verify that the first section on the right reads ‘Windows Server 2008 R2 Standard’.

 © 2017 SAM

Upgrading

When upgrading from versions prior to V5.4 rev 8, note the following registry settings.

Registry Settings

Under its development name, the Media Transformer was previously known as the QTube Transformer in versions prior to V5.4 rev 8. Software settings are saved in the Window's Registry under a key called **QTube Transformer**.

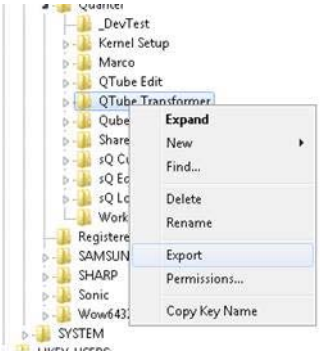

Figure 1 AJA Devices

From release V5.4 rev 8 onwards, the key is called **Media Transformer**. Any existing registry settings must be migrated from the **QTube Transformer** key to the **Media Transformer** key.

1. Open **regedit.exe**.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Quantel\QTube Transformer**.
3. Right-click and select **export**.
4. Export this to a temporary folder.
5. Open this exported file in a text editor.
6. Within the text editor, perform a find and replace from string '**\SOFTWARE\Quantel\QTube Transformer**' to '**\SOFTWARE\Quantel\Media Transformer**'.
7. Save the changes to the file.
8. Back in **regedit.exe**, import the edited file.

This migrates the registry settings from **QTube Transformer** to **Media Transformer**.

 © 2017 SAM

Media Transformer Setup

Configure Operating System

The operating system must have specific settings applied to ensure all software components are linked together:

Switch on Jumbo Packets

1. From the **Start** menu, open the **Control Panel**.
2. Select **Hardware and Sound**.
3. In the **Devices and Printers** section, select **Device Manager**.
4. Click on the arrow to the left of **Network adapters** to expand it.
5. Right-click on the adapter pointing to the ISA and sQs (**quanet**) and select **Properties**.
6. Select the **Advanced** tab.
7. In the **Settings** list select **Jumbo Packet**.
8. Using the **Value** drop-down, select **9014**.
9. Click **OK**.

The cluster adapter remains on the normal 1500 MTU setting.

Turn off Firewall

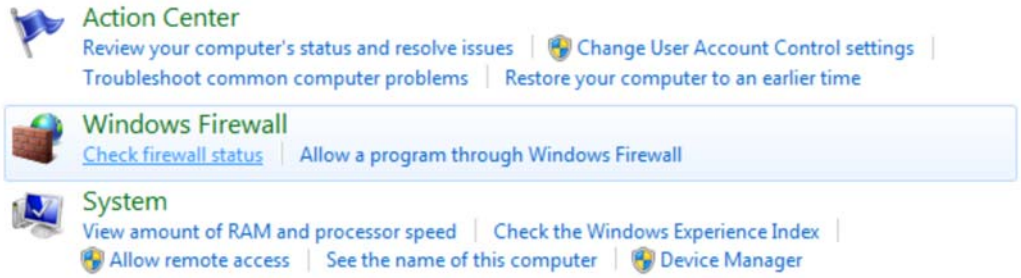

Figure 2 AJA Devices

1. From the **Start** menu, load the **Control Panel**.
2. In the **System and Security** section, select **Check firewall status**.
3. In the left panel, select **Turn Windows Firewall on or off**.

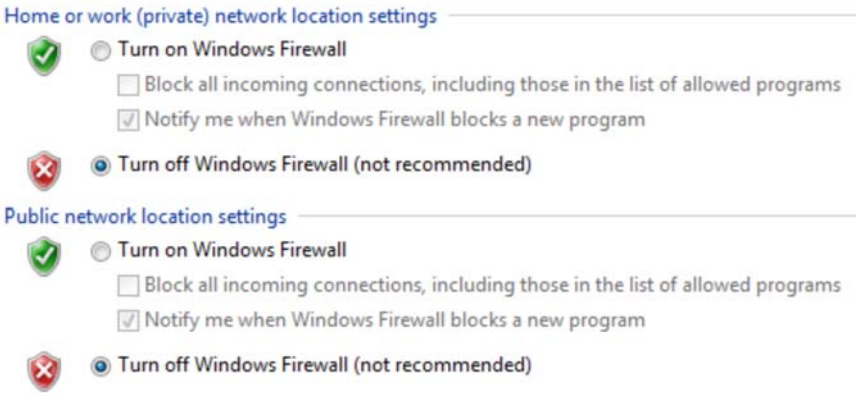

Figure 3 AJA Devices

 © 2017 SAM

4. In **Home or work (private) network location settings**, select **Turn off Windows Firewall (not recommended)**.
5. In **Public network location settings**, select **Turn off Windows Firewall (not recommended)**.
6. Click **OK**.

Install Transformer Software

1. On the Transformer PC, login as Windows administrator and double-click the downloaded setup.exe file (alternatively, right-click the .exe file and select **Run as administrator**). This starts the Setup wizard.
2. Select **Media Transformer** from the product drop-down box and click **Install** in the bottom-right of the window. The end user license agreement then displays.
3. Read this carefully and then click **Agree** to accept the license agreement. The software now installs: this may take a few minutes.
4. Tick **Run now** and **Create shortcut on the Desktop** and then click **OK** in the bottom-right of the window. The software now starts.
5. When the software has finished loading, press <Ctrl>+<F9> to close the software.

Running the software for the first time (step 4 above) is important as it populates the default registry settings.

License

Obtain License using Disk ID

1. Navigate to **C:\Data\Logs** and open the file named **Recent**. This opens the most recent activity log.
2. Press <Ctrl>+<F> to open the search tool.
3. Search the log for the phrase: **Valid locking code**.
4. E-mail this code to **licences@s-a-m.com**, quoting the order number and allow one working day for the license to be created and mailed.
5. When the license has been received, install it using the steps below.

Install License

To install the license:

1. In Windows, create the directory **C:\Data\Licenses**.

Ensure that the 'licenses' folder is spelt as shown above in order for it to be correctly located by the software.

2. Place the supplied **lservrc.lic** license file in this directory.

 © 2017 SAM

Transformer Settings

After installing the license, settings must be configured in the Settings menu. Some settings are not described here, as they are optional, depending on user preference.

1. In Windows, navigate to: **Start – All Programs – SAM – Media Transformer V#.# rev # – Settings**.
2. Right-click **Settings** then select **Run as administrator**.

Some of these options only become available after running the software up for the first time.

The scroll box at the top-left of the Settings application provides access to different menus:

License

1. From the top-left drop-down box, select **License**.

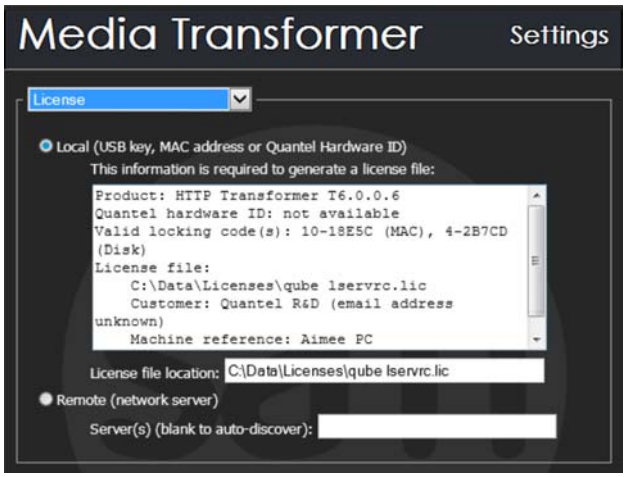

Figure 4 License

2. Select **Local**.
3. Check that the License file location path is **C:\Data\Licenses\lservrc.lic**.

Network

1. From the top-left drop-down box, select **Network**.

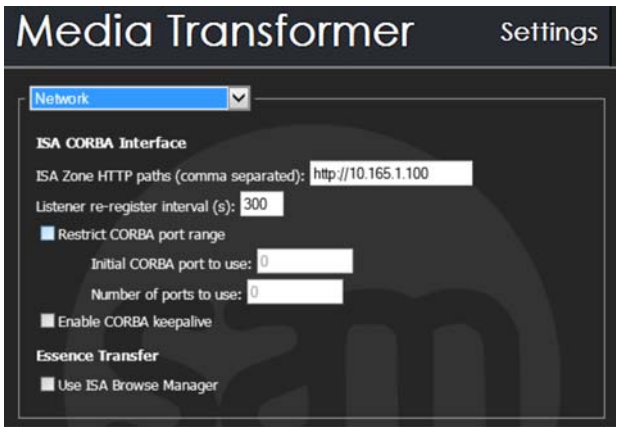

Figure 5 Network

 © 2017 SAM

2. In the **ISA Zone HTTP paths** field, enter the location of the ISA Manager's ZonePortal IOR e.g., **http://my-isa/ZoneManager.ior**.

3. Deselect **Essence Transfer – Use ISA Browse Manager**.

Network: Clipnet

1. From the top-left drop-down box, select **Network: Clipnet**.

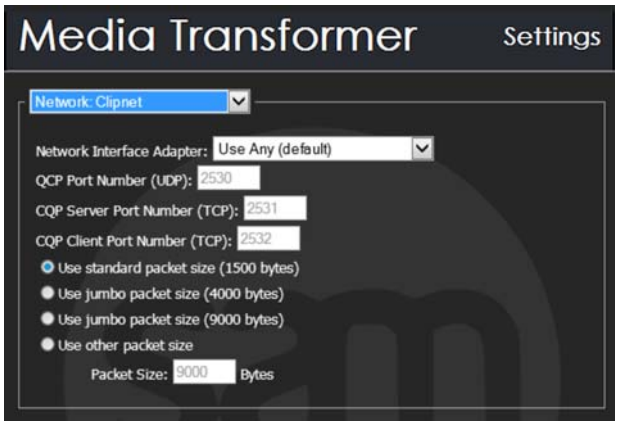

Figure 6 Network:Clipnet

2. Set **Network Interface Adapter** to **quanet**.

3. Select **Use jumbo packet size (9000 bytes)**.

Options

If there is video encoded as DV100 or AVCI on the server, then the relevant licence checks need to be enabled:

1. From the top-left drop-down box, select **Options**.

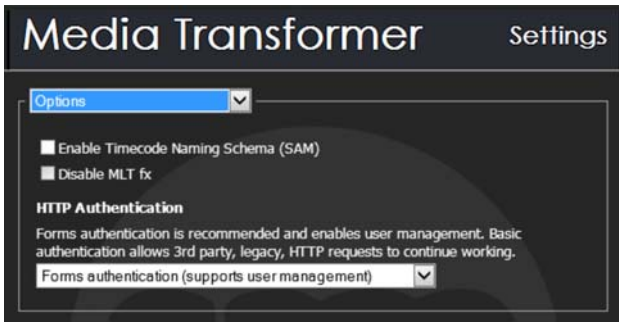

Figure 7 Options

2. Tick either **Enable AVCI decode licence**, **Enable AVCI encode licence check** or **Enable DV100 license check** (depending on sQ formats enabled).

 © 2017 SAM

HTTP

The web interface defaults to port 80 which is already in use by IIS so it must be changed:

1. From the top-left drop-down box, select **Http Server**.

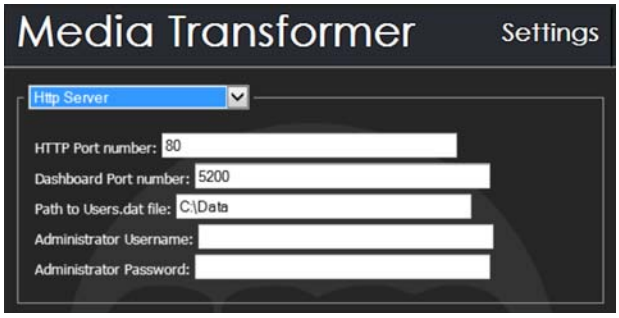

Figure 8 HTTP Server

2. Set **HTTP Port number to 8080**.

Startup

1. From the top-left drop-down, select **Startup**.

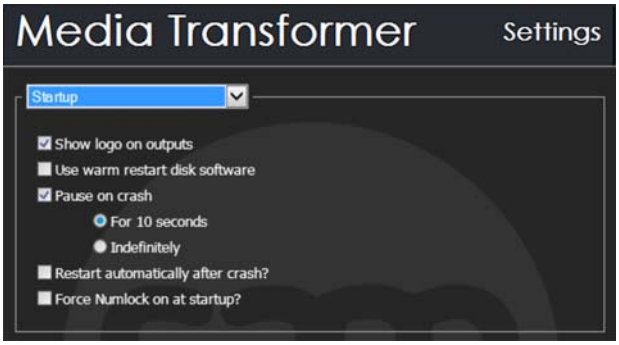

Figure 9 Startup

2. Deselect **Pause on crash**.
3. Select **Restart automatically after crash?**.

QTube Settings

Setting a Mixed Browse System

If there is a mixture of clip formats being used in the system (e.g. MPEG-1 browse and H.264) the Media Transformer can be set to browse mixed formats.

1. From the top-left drop-down, select **QTube Settings**.

 © 2017 SAM

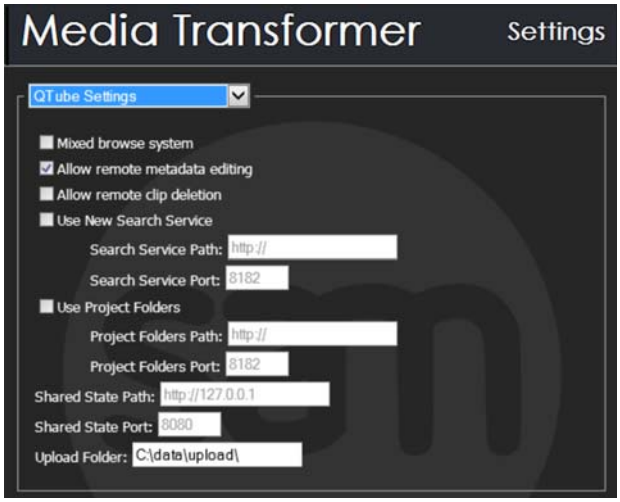

Figure 10 QTibe Settings

2. Select **Mixed browse system**.

Allow Metadata Editing

To be able to edit metadata in the QTube Browser and QTube Edit:

1. From the top-left drop-down, select **QTube Settings**.
2. Select **Allow remote metadata editing**.

Allow Clip Deletion

Whilst clips cannot be deleted from the QTube Browser, they can be deleted from QTube Edit. To enable this:

1. From the top-left drop-down, select **QTube Settings**.
2. Select **Allow remote clip deletion**.

Server: Search

Media Transformer settings allow search constraints to be set up on any connected client. To set up a search constraint:

1. From the top-left drop-down, select **Server: Search**.

Figure 11 Server Search

2. Enter a constraint in the **Search Constraint** field.

Constraints take the form:	+AND+Metadata Type:Constraint
For example:	+AND+Title:Recording

 © 2017 SAM

This example means that there is a search constraint that only allows users to search among clips that have ‘Recording’ as all or part of the title.

3. After entering the constraint in the **Search Constraint** field, click **OK**.

Essence: Audio

If the Transformer does not have a dedicated audio disk partition set the audio folder to a drive partition which has sufficient space to store audio for clips published via QTube. Transformer PCs supplied have enough space in the Data Partition to set this up.

1. From the top-left drop-down box, select **Essence: Audio**.

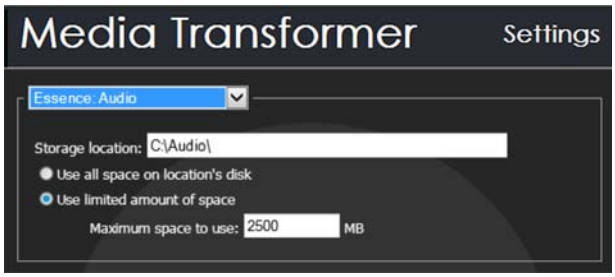

Figure 12 Essence Audio

2. Ensure that the **Storage location** is set to **C:\Data\Audio**.
3. Tick **Use limited amount of space**. A default maximum space to use is assigned.
4. (Optional) Assign a sensible maximum space to be used for audio storage. For example, 15 GB audio space provides about two hours and forty-five minutes of 8-channel audio (figures are based on PAL system). This requires approximately 15360 MB to be allocated for audio storage.

 © 2017 SAM

Essence: Video (PC)

If the Transformer does not have a dedicated video disk partition set the video folder to a drive partition which has sufficient space to store video for clips published via QTube. Transformer PCs supplied have enough space in the Data Partition to set this up.

1. From the top-left drop-down box, select **Essence: Video (PC)**.

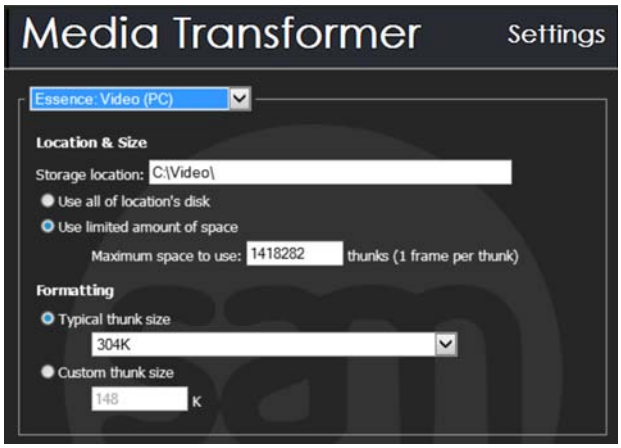

Figure 13 Essence Video

2. Ensure that the **Storage location** is set to **C:\Data\Video**.
3. Tick **Use limited amount of space**. A default maximum space to use is assigned.

(Optional) Assign a sensible maximum number of thunks to be used for video storage. For example, 51 GB provides space for approximately one hour of HD 100 Mbit data and two hours of SD IMX or DVCPro data. This requires approximately 95000 thunks to be allocated for video storage.

Setting Group Area Constraints

On the Transformer it is possible to set up exclusive areas for specific groups of users. For example, a specific area could be set up to be exclusively available to lead editors. The specific areas can be set up via the ISA manager. Setting group access through the Transformer affects all connected clients. To set up group access:

1. Open a file browser on the Transformer and navigate to the path: **SAM – Media Transformer\Quantel\QuentinCorba\<Version Number>\Custom Settings\Config**.
2. Double-click on **Allowed Publish Groups** in the right-hand panel.
3. Enter the group value in the **Value data** field (e.g. Editors).
4. Click **OK**.
5. Restart the Transformer PC.

 © 2017 SAM

IIS and Couch DB Setup

Install IIS and CouchDB

1. In the **C:\Data\<Transformer>\DLL_Data\Quantel\QCIFSBin\iis-support**, unzip the **TransformerBuild.zip** and run **LaunchMeAsAdministrator.bat**.
2. In order to verify, unzip **CheckConfig.zip** and run **LaunchMe.bat**.

Security

About Certificates

These settings depend on each organization's setup and there are several security options that can be chosen. These instructions describe how to create a self-signed certificate and then share it with any other machines in the cluster. A self-signed certificate is free to create and use.

The effect of this is that new visitors to the site are informed that it is a valid certificate but it has not been verified by a trusted site. This notification must be accepted and then the certificate must be saved locally.

It is the responsibility of each organization to arrange a server certificate from a 'Trusted Authority' should one be required. SAM cannot apply for one on another organization's behalf (a restriction put in place by the signing authority). On receipt, it can be imported using the instructions below.

Certificate Creation

The certificate must be created on one PC and then imported to all others. To create self-signed certificates and then export:

1. **Go to Start – All Programs – Administration Tools – Internet Information Services (IIS) Manager**.
2. In the **Connections** panel, highlight the hostname (hostname\administrator). For example, **PVGIS-CC01 (PVGIS-CC01\quantel)**.
3. Double-click **Server Certificates** and select **Create Self-Signed Certificate...**

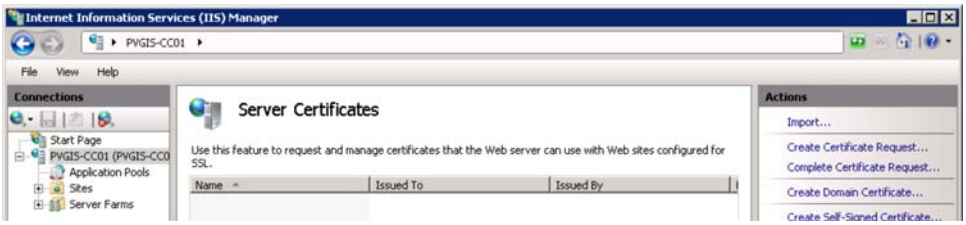

Figure 14 Essence Video

4. In the **Specify a friendly name for the certificate** field, enter the domain name of the cluster.
5. Click **OK**.
6. From the **Actions** panel on the right, highlight the new certificate and click **Export...**
7. In the **Export to** field enter **C:\<cluster-name>**.
8. Enter a password into the **Password** and **Confirm password** fields.
9. Click **OK**.
10. Open Windows Explorer and navigate to where the certificate is stored and copy it to somewhere centrally available.

 © 2017 SAM

Install Certificates on Each Client

The certificate must be installed on each client PC, otherwise authorisation is required each time the client PC is used. To import the certificate:

1. Go to **Start – All Programs – Administration Tools – Internet Information Services (IIS) Manager**.
2. In the **Connections** panel, highlight the hostname (hostname\administrator). For example, **PVGIS-CC01 (PVGIS-CC01\quantel)**.
3. Double-click **Server Certificates** and select **Import...** from the Actions panel.
4. Navigate to the shared location of the PFX file and enter the password it was created with.
5. Click **OK**.

When a certificate has been created or imported it must be 'bound' to the relevant port:

1. Go to **Start – All Programs – Administration Tools – Internet Information Services (IIS) Manager**.
2. In the **Connections** panel, highlight the hostname (hostname\administrator). For example, **PVGIS-CC01 (PVGIS-CC01\quantel)**.
3. Expand **Sites** and highlight **Default Web Site**.

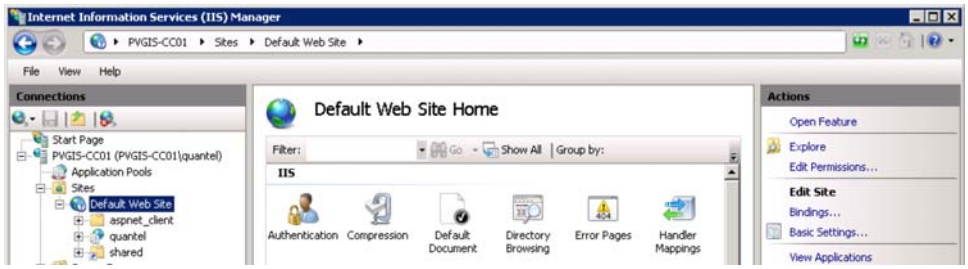

Figure 15 Essence Video

4. Select **Edit Site – Bindings...** from the **Actions** panel on the right.
5. If all testing is finished, select **http** from the list of Site Bindings and click **Remove**.
6. Click **Add...** to add site bindings.

Figure 16 Essence Video

7. Set **Type** to **https** and set **IP address** to **All Unassigned**.
8. Set **Port** to **443** (for https).
9. Set **SSL Certificate** to the installed certificate and click **OK**.

 © 2017 SAM

Authentication

1. Launch the IIS Manager program. Go to **Start – All Programs – Administration Tools – Internet Information Services (IIS) Manager**.
2. In the **Connections** panel, highlight the hostname (hostname\administrator). For example, **PVGIS-CC01 (PVGIS-CC01\quantel)**.

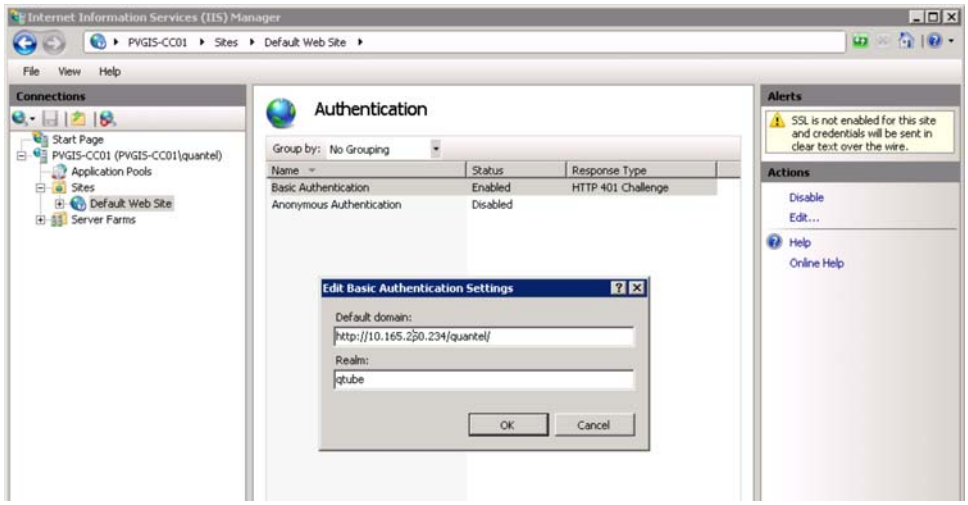

Figure 17 Essence Video

3. Double-click **Authentication** from the central panel.

When utilizing Remote User Management:

1. Right-click on **Anonymous Authentication** and select **Enable**.
2. Right-click on **Basic Authentication** and select **Disable**.
3. Right-click on **Form Authentication** and select **Enable**.
4. Click **OK**.

 © 2017 SAM

Search Service Setup

Do not install the search service on the ISA Manager.

Search Service Overview

Each Zone that has a Media Transformer attached to it requires a Search service. The Search service is a separate zipped package (**Search V2.0.1.0.zip**) which can be installed on any PC or on the Transformer, but must not be installed on the ISA Manager.

Any changes made to the ISA Manager may seriously impact workflow and system network traffic. DO NOT change any settings unless you are a qualified engineer. Always contact SAM 24-hour support for advice beforehand.

Web Server Port

By default, the Search service starts on port 8182. This setting can be changed by editing the attribute **webserverPort** in the configuration file. The configuration file for the Search service is located at **webserver/quantel/config.xml**. As a shortcut, execute **bin/configure.bat**.

```
<?xml version="1.0"?>
<config>
    <!-- REST Web service configuration file -->
    <webserverPort>8182</webserverPort>
    <isa>
        <!--Comma-separated list of ISA Managers IOR URLs. At least one entry must be specified.-->
        <URLs>http://localhost:80</URLs>
        <!--Name of an ISA Manager database user with at least read-only priviledges on the clips table.-->
        <user>quantel</user>
        <!--Password of the database user mentionned above.-->
        <password/>
        <!--How long (in seconds) to wait between attempts to connect to the ISA Manager.-->
        <connectionRetryTimeout>10</connectionRetryTimeout>
        <!--How often (in seconds) to expect to hear from the ISA Manager.-->
        <heartbeatPeriod>10</heartbeatPeriod>
    </isa>
    <searchService>
        <!--URL of a Solr server to use for data indexing and searching.-->
        <solrURL>http://localhost:${webserverPort}/solr</solrURL>
        <!--Filter out accents in ISOLatin1 Characters prior to search.-->
        <filterISOLatin1Characters>true</filterISOLatin1Characters>
        <!-- Use this section to store arbitrary properties. The Search Service will store those properties and make them available via its RESTful API. -->
        <meta> </meta>
    </searchService>
</config>
```

Figure 18 Essence Video

ISA Settings

The Search service can only index one ISA Zone. The Search service must be configured with the URL of an ISA in that Zone. An ISA master/slave URL pair can also be specified. Given an ISA URL in the form **http://[host]:[port]/ZoneManager.ior** the Search service attempts to fetch the IOR at the following **URL: http://[host]:[port]/ZoneManager.ior**.

The Search service also requires the appropriate user name and password for accessing the ISA database via JDBC.

Customise Log Output

The log output of the Search service can be customized before it is started. This can be done by overriding the logback configuration file located at **webserver/quantel/extra/logback.xml**. By default, log files are produced under the folder **webserver/logs**.

 © 2017 SAM

Install Search Service

Installation

To install the search service:

1. Add the ISA Master and slave to the machine's HOST file that is running the search service.
2. Extract the Search service zip and copy the folder to **c:\Data**.
3. Rename the folder '**search**'.
4. In the **search** folder is a folder called **bin**. Open this and run **addshortcuts.bat**. This creates a folder on the desktop with shortcuts.
5. Browse to the shortcut folder on the desktop and run **configure.bat**.
6. Add the ISA Master and slave address in the following URLs:
   http://10.165.26.10:80
   http://10.165.26.11:80
7. </URLs><bindAddress>local_IP_Address</bindAddress>
   The local IP address should be the IP address of the network adapter that the Search Service PC uses to connect to the ISA Manager.
8. Check the **config** file to make sure no other settings need to be changed for a site specific install. In most of cases nothing needs to change.
9. Save and close the **config** file.
10. Run **start_search.bat**.
11. Enter the following URL into a web browser. This must be done on the machine where the search service is running.
    http://localhost:8182/quantel/search/select?q=*

    An XML formatted page with a list of clips displays.

In case of issues with running the search service, the logs are located in the following file path:

c:\Data\Search\Search\webserver\logs

Search Service Access

Ensure that the property 'SearchPath' in the ISA Manager is set to the location of where the Search service resides so that it can be found by the QTube Transformer For example, if the Search service PC's IP address is **10.10.10.10** then the path should be set to: **http://10.10.10.10:8182/**. To set up the 'SearchPath':

1. On the ISA Manager web interface, navigate to **Configure – Properties**.
2. In the **Property** column, locate **searchpath:**
   - If the **searchpath** property doesn't exist, create and configure it by following steps 3 - 6.
   - If the **searchpath** property exists but is not set correctly, update the existing setting by selecting **searchpath**. Edit the settings by following steps 4 - 6.
3. Press **Add property** and set the name as '**searchpath**'.
4. Set the value to the following:
   http://{IP address of search service}:8182/
5. Press **searchpath** and enter the correct IP for the search service.
6. Press **Create** and then **Refresh database** at the top of the page.

 © 2017 SAM

The Search service can be controlled by tools located under the bin folder. Most tools use the search.bat command line interface. Execute **search.bat -help** for some help messages on how to use it.

The Search service needs to be running, in order to populate the server bin with clips. Execute **bin\start_search.bat** to start the Search service.

The Search service is ready when **“- Waiting for an indexing operation to be submitted.”** has been displayed in the console window.

To check that the Search service is running, open the following URL:

http://localhost:[port]/quantel/search/select?q=*

Alternatively, execute **search -status**.

Execute **stop_search.bat** or **search -stop** to stop the Search service.

 © 2017 SAM

Load Balancer Configuration

Install and configure Internet Information Services (IIS) with Application Request Routing (ARR) and Windows Network Load Balance.

This example is based on using X8 Supermicro Servers with 32 GB RAM installed and dual 10 Gb NICs (X520-2). For the configuration 1 Gb NIC from each server is used for management and RDP.

Server A win 2012 R2 Datacenter

1 Gb NIC 10.165.190.160 - no gateway configured

10 Gb NIC10.165.185.160 - JumboFrames enabled and with gateway configured

Server B win 2012 R2 Datacenter

1 Gb NIC 10.165.190.161 - no gateway configured

10 Gb NIC10.165.185.161 - JumboFrames enabled and with gateway configured

NLB Cluster IP Address **10.165.185.163**

On both servers an account with same username and password with administration privileges is required.

Disable the firewall on all profiles for both servers.

Install and Configure NLB

Add Network Load Balancing Tools Feature to Server A and Server B

1. Open **Server Manager - Add Roles and Features** and select **Features.**
2. Expand **Remote Server Administration Tools**.
3. Expand **Feature Administration Tools**.
4. Select **Network Load Balancing Tools**.

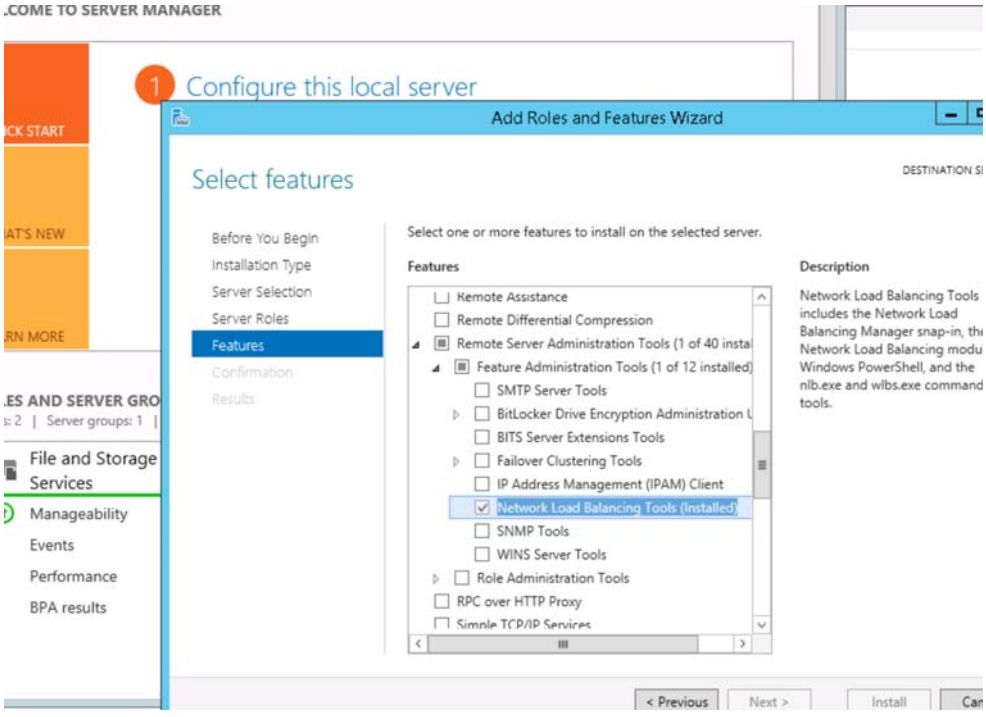

Figure 19

5. Install and wait for the service to become available.

 © 2017 SAM

Configure the Cluster

Check that the NLB feature is installed on both servers before proceeding further.

NLB is configured using the NLB Manager from one of the servers but this completes the NLB cluster configuration on both servers.

1. From one of the servers start the command prompt and type **nlbmgr**
2. Open NLB Manager window and click **Options - Credentials** and enter the admin username and password previously created on both servers.
3. Go to **Cluster - New** and in the **Host** field type the IP address of Server B, for example.

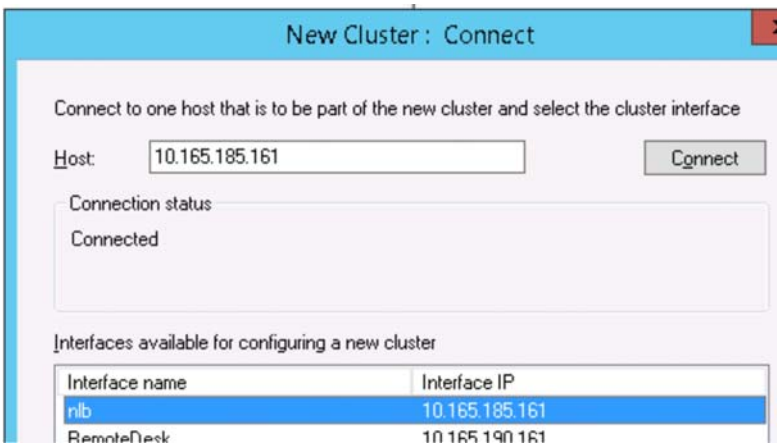

Figure 20 Essence Video

4. Select NLB interface 10.165.185.161 and click **Next**.
5. Click **Next** again.
6. In **New Cluster: Cluster IP Address** window click **Add**.
7. Enter the IP address of the cluster and the subnet mask.

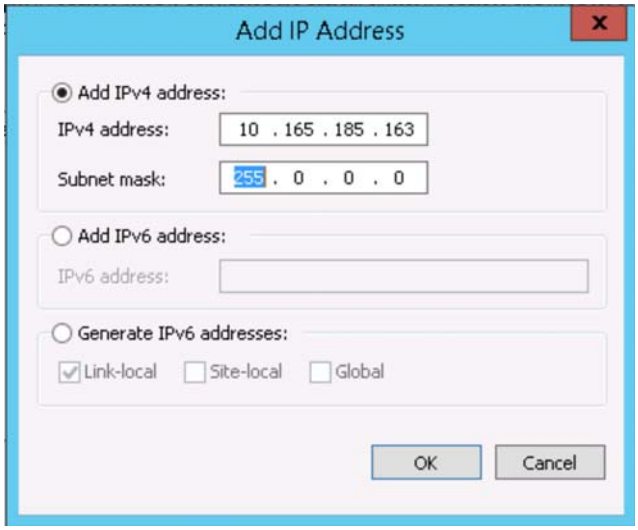

Figure 21

8. Click **OK**.
9. Click **Next**.

 © 2017 SAM

10. In **New Cluster: Port Rules** window click **Edit** and use the following screenshot as a reference for configuring the Port Rules.

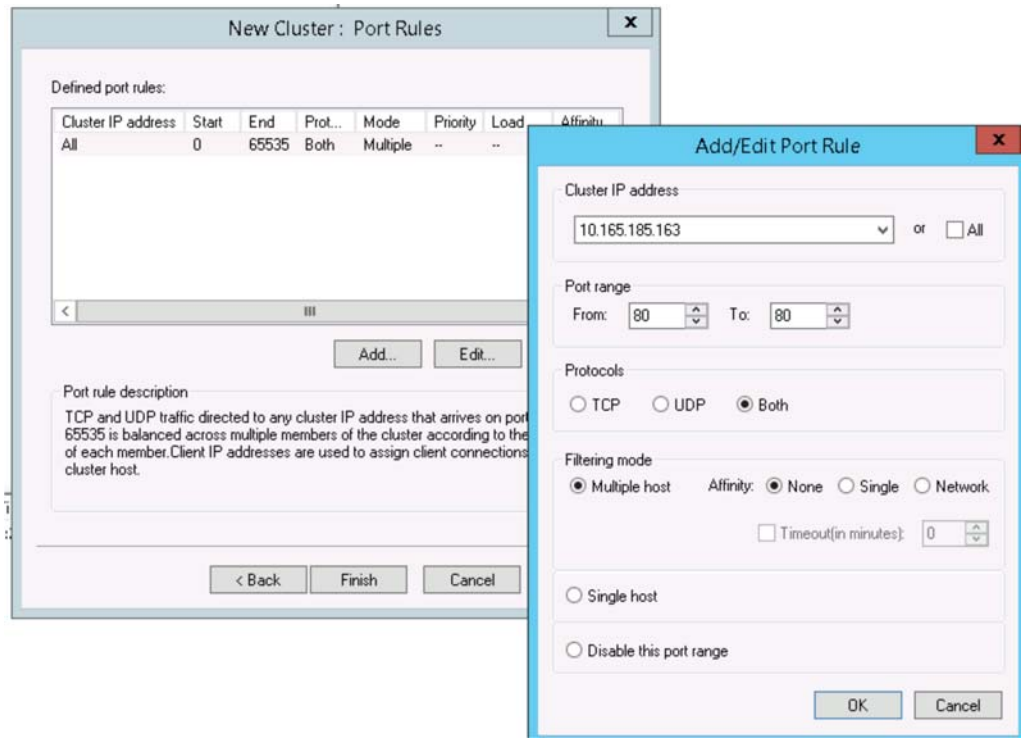

Figure 22

11. Click **OK**.
12. Click **Finish**.

The NLB cluster is configured. After approximately one minute the NLB Manager window displays the server B (NLB2) status as **Converged**.

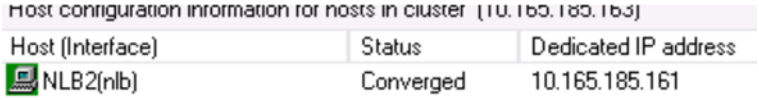

Figure 23

Now add Server A to the Cluster.

13. Go to **Cluster - Add Host** and repeat the same steps as for the configuration of server B previously.

After configuring server A in the NLB Manager window the cluster status will be as follows:

Figure 24

From another PC, ping the IP address of the cluster. A successful reply confirms the NLB cluster is configured correctly.

 © 2017 SAM

Install and Configure IIS

Add the Web Server (IIS) Role to the Servers

- Go to **Server Manager - Add Roles and Features** and select **Web Server (IIS)**

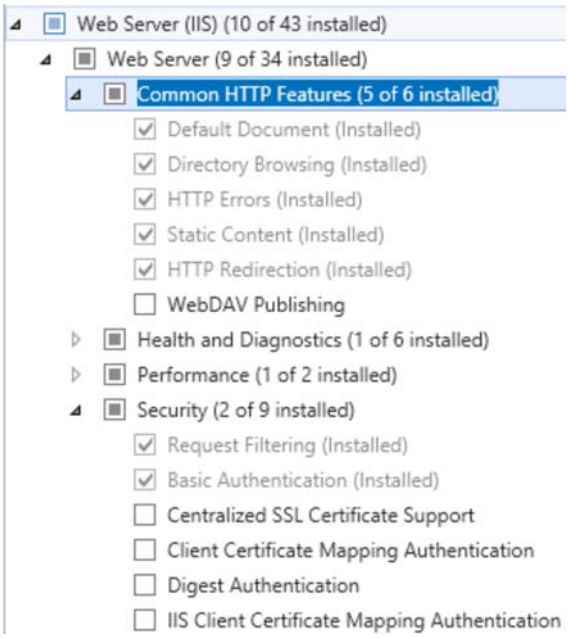

Figure 25

Configure IIS Shared Configuration on Server A and Server B

Open the **Internet Information Services (IIS) Manager** and open **Shared Configuration**.

- Enable this feature by ticking the box. Then define a physical path where the configuration files and encryption keys will be stored.

The example in the following screenshot uses the username of the local administrator. Set a random encryption password that must be remembered in order to configure the second server to use IIS with a shared config.

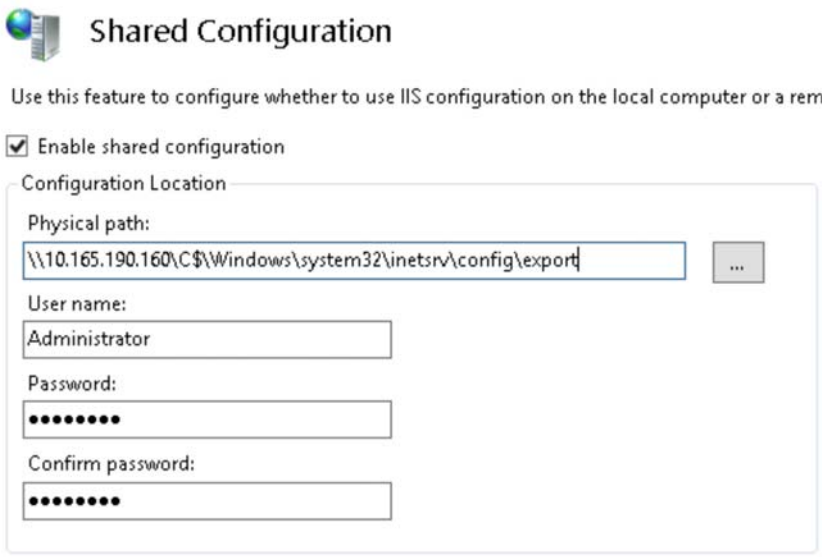

Figure 26

- Enable Shared Configuration on the second server and use the same Physical path, same username and password and same encryption key pass.

 © 2017 SAM

Change Default Web Site Bindings

Open **Default - Bindings - select http protocol** - click **Edit** and add the ip cluster IP address and port 80.

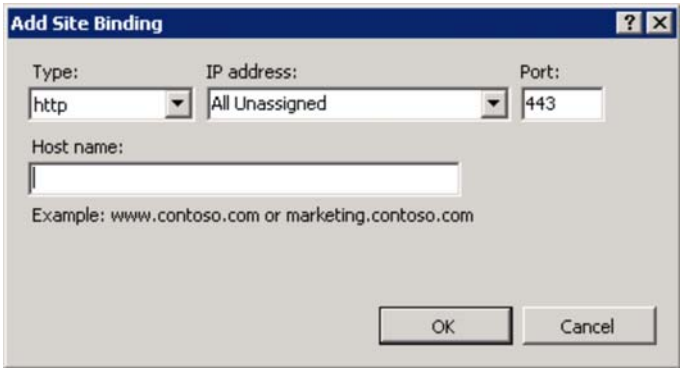

Figure 27

From the other server check that the Bindings are the same as on the server that has been changed.

Installing ARR manually without WebPI

ARR must be installed on both servers

Microsoft's Application Request Router (ARR) IIS Extension is a complex piece of software which integrates with several other components to do its job. These components are URL Rewrite, Web Farm Framework and ARR's External Cache module. For everything to work correctly, all components must be installed in a specific order. Several years ago, Microsoft introduced the Web Platform Installer (WebPI) mechanism, which makes it easy to manage installed components, and this is a good way to install ARR and all its components properly.

Occasionally, there may be reasons to no use the WebPI installation option. For example, when installing ARR on the Server Core edition of Windows, where WebPI cannot be used. If so, another option is installing it using the IExpress package, which includes all the components together. To use this, download it from *www.microsoft.com*.

A further option is to install the components manually, which requires all components to be downloaded separately from *www.microsoft.com*:

1. Firstly, Stop IIS. From a command prompt, type **net stop was /y** and **net stop wmsvc /y**:

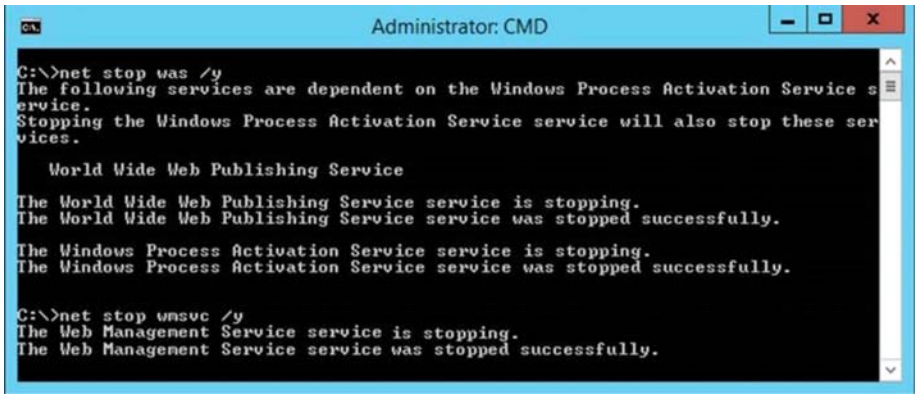

Figure 28

WMSVC is the IIS Web Management Service, which may not be enabled on the server. If it is not enabled, "The Web Management Service service is not started." displays. This warning can be ignored.

 © 2017 SAM

2. Download and install the Web Farm Framework module.
3. Download and install the External cache module.
4. Download and install the URL Rewrite module.
5. Download and install ARR itself.
6. Restart the IIS services (or, reboot the server).

If downloading to an X86 server, for example, windows 2008, download the X86 version of these components.

Configure ARR

1. Open IIS Manager on one server and open Application Request Routing Cache.

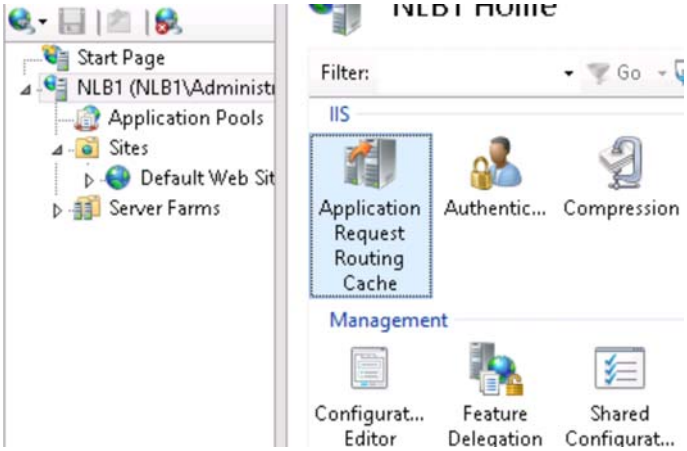

Figure 29

2. In the right panel click **Server Proxy Settings**.

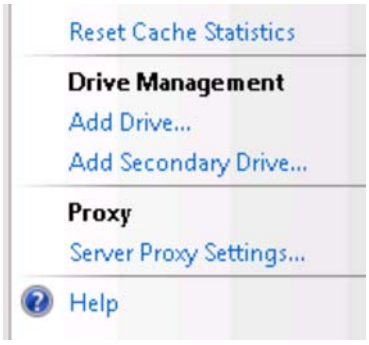

Figure 30

3. Tick **Enable the Proxy**.
4. Click **Apply** from the right panel in the **Action** section.

From the other server check that the Server Proxy Settings are the same as on the server that has been changed.

 © 2017 SAM

Create and configure a Server Farm

1. Open IIS Manager and on Server Farms Create New Server Farm.

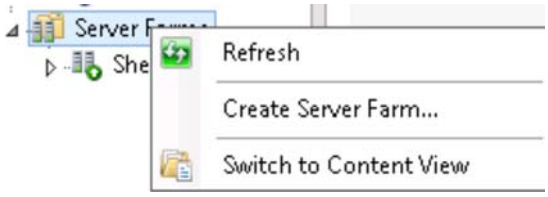

Figure 31

2. Type a name for the New Server Farm and click **Next**.

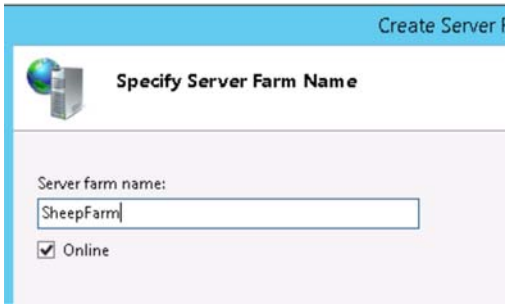

Figure 32

3. Add the ip addresses of the machines to be part of the web farm (machines behind the load balancer).
4. Click **Add** to add a new machine and **Finish** once the list of servers is complete.
5. Click **Yes** to create the appropriate rewrite rules.

Figure 33

6. Once finished, inspect the servers in the IIS Manager by expanding the Server Farms tree down to the Servers section.

 © 2017 SAM

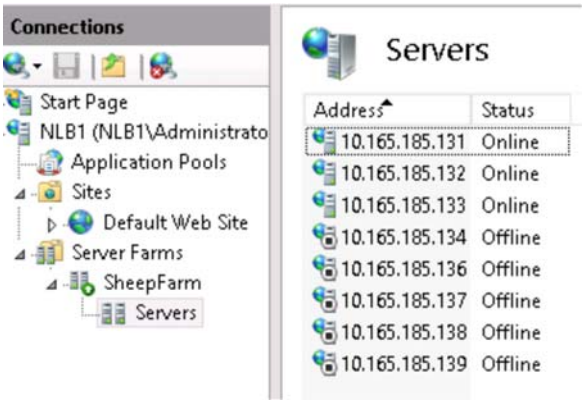

Figure 34

7. Click on the name of the farm to display the options available for configuring the Farm

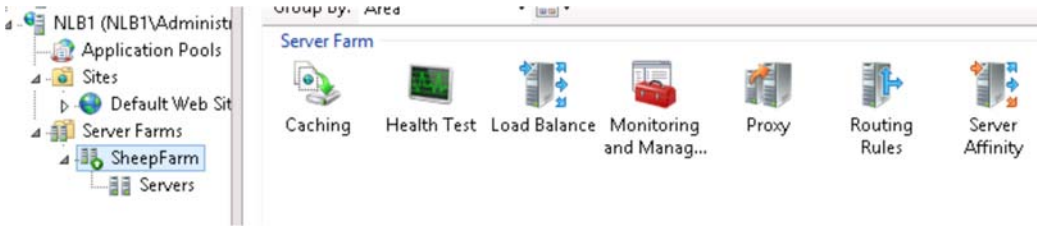

Figure 35

Configure the Server Farm options according to the following screenshots, clicking **Apply** on the right-hand side of the screen after each change:

Configure Caching

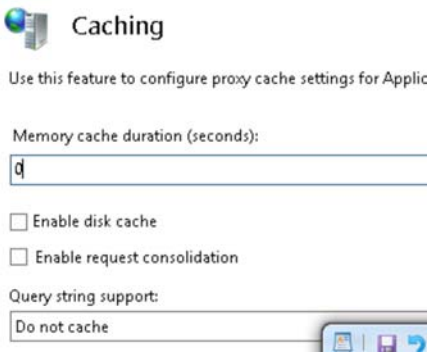

Figure 36

 © 2017 SAM

Configure Health Test

Figure 37

The URL Test has the IP Address of the CLUSTER 10.165.185.163 previously configured on NLB cluster.

Configure Load Balance

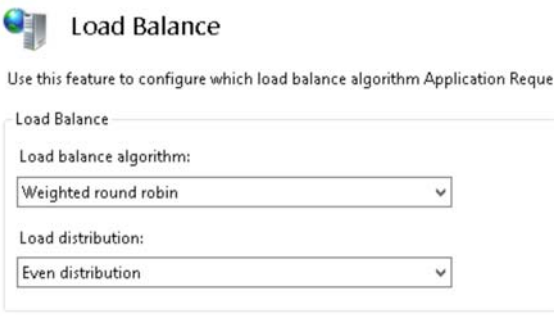

Figure 38

 © 2017 SAM

Configure Proxy

Figure 39

Configure Routing Rules

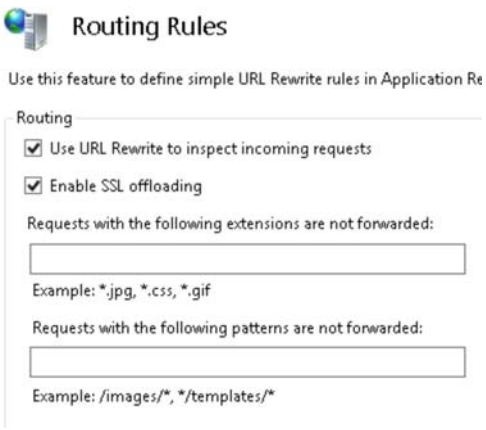

Figure 40

 © 2017 SAM

Configure Server Affinity

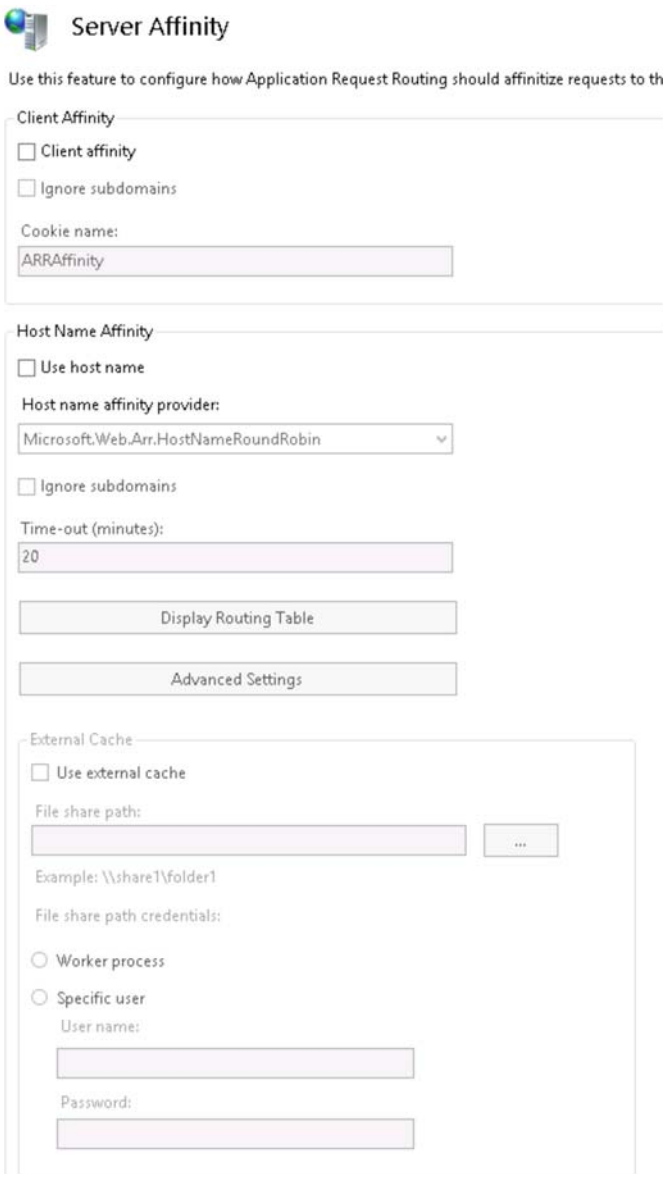

Figure 41

To test the Transformer cluster use the URL *http://10.165.185.163/quantel* where the IP address "10.165.185.163" is the IP address of the NLB Cluster.

 © 2017 SAM

Force LBR Pass-through

This setting allows administrators of a Transformer system to force all SAM VIBE clients that connect to use LBR pass-through. LBR pass-through requires that the sQ stores browse as H264. LBR pass-through means that much less CPU is used when streaming a clip in SAM VIBE and so a Transformer can support up to 20 clients connected to it instead of 4. However, it does mean that clients lose the adaptive bitrate functionality meaning that they must ensure they have at least enough bandwidth to stream the native browse from the Transformer. For normal H264 browse, this should be at least 4 Mb/s.

In order to force LBR Pass-through on all clients accessing a transformer:

1. Open **C:\inetpub\wwwroot\go\config.txt**
2. Add the following:

```
"passThrough":{
    "override":true,
    "value":true

},
```

3. Save the file to another folder (e.g. Documents)
4. Copy the file back to the ...go folder.

Create and Configure Rewrite Rules

Configuring URL Rewrite

There are some URL Rewrite rules you need to configure on a load balancer in order to ensure certain operations will work correctly. Do the following:

- On the load balancer, open IIS Manager.
- In the left pane, labelled **Connections**, click on the name of the server (eg. WIN-LRRF990fAF\quantel)
- In the right pane select **URL Rewrite**.
- You now need to add a set of rules. Repeat this process for each rule:
  - On the far right select **Add Rule**(s).
  - Select **Inbound rules** -> **Blank rule**. Click **OK**.
  - Give the rule a unique name, add the values below, and click **Apply**.

Create the following rules:

- Name: **HTTPS Rewrite**
- Requested URL: **Matches the Pattern**
- Using: **Wildcards**
- Pattern: ***
- Ignore case: **True**
- Logical grouping: **Match Any**
- Conditions:
  - Condition input: **{QUERY_STRING}**
  - Check if input string: **Matches the Pattern**
  - Pattern: **HTTPS**
  - Ignore case: **True**

 © 2017 SAM

- Server Variables:
  - Server variable name: **SERVER_PORT_SECURE**
  - Value: **HTTPS**
  - Replace the existing value: **True**
- Action type: **Rewrite**
- Rewrite URL: **{R:1}**
- Append query string: **TRUE**
- Stop processing of subsequent rules: **FALSE**

- Name: **StickySession**
- Requested URL: **Matches the Pattern**
- Using: **Wildcards**
- Pattern: ***quantel*;redirect=*;***
- Ignore case: **TRUE**
- Logical grouping: **Match Any**
- Conditions: **None**
- Server Variables: **None**
- Action type: **Rewrite**
- Rewrite URL: **http://{R:3}/quantel/{R:2}{R:4}**
- Append query string: **TRUE**
- Stop processing of subsequent rules: **TRUE**

- Name: **ARR_ServerFarm_HTTP**
- Requested URL: **Matches the Pattern**
- Using: **Wildcards**
- Pattern: ***
- Ignore case: **TRUE**
- Logical grouping: **Match Any**
- Conditions: **None**
- Server Variables: **None**
- Action type: **Route to Server Farm**
- Action Properties:
  - Scheme: **http://**
  - Server farm: **<Name of server farm>**
  - Path: **/{R:0}**
- Stop processing of subsequent rules: **FALSE**

- Name: **ARR_SocialMediaDelivery_HTTP**
- Requested URL: **Matches the Pattern**
- Using: **Wildcards**
- Pattern: ***share**
- Ignore case: **TRUE**

 © 2017 SAM

- Logical grouping: **Match Any**
- Conditions: **None**
- Server Variables: **None**
- Action type: **Route to Server Farm**
- Action Properties:
  - Scheme: **http://**
  - Server farm: **<Name of server farm for social media>**
  - Path: **/{R:0}**
- Stop processing of subsequent rules: **FALSE**

 © 2017 SAM